

HOUSE BILL 3115

By Kernell

AN ACT to enact the Tennessee Privacy Protection Act of 2000.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. The title of this act is, and may be cited as the "Tennessee Privacy Protection Act of 2000".

SECTION 2. Definitions. As used in this act:

(a) The term "information system" means the total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the global information system known as the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.

(b) The term "personal information" means all information that describes, locates or indexes anything about an individual including his or her real or personal property holdings derived from tax returns, and his or her education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his or her

presence, registration, or membership in an organization or activity, or admission to an institution. The term does not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information.

(c) The term "data subject" means an individual about whom personal information is indexed or may be located under his or her name, personal number, or other identifiable particulars, in an information system.

(d) The term "disseminate" means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means.

(e) The term "purge" means to obliterate information completely from the transient, permanent, or archival records of an organization.

(f) The term "agency" means any agency, authority, board, department, division, commission, institution, bureau, or like governmental entity of the state or of any unit of local government including counties, cities, towns and regional governments and the departments and including any entity, whether public or private, with which any of the foregoing has entered into a contractual relationship for the operation of a system of personal information to accomplish an agency function. Any such entity included in this definition by reason of a contractual relationship shall only be deemed an agency as relates to services performed pursuant to that contractual relationship, provided that if any such entity is a consumer reporting agency, it shall be deemed to have satisfied all of the requirements of this chapter if it fully complies with the requirements of the Federal Fair Credit Reporting Act as applicable to services performed pursuant to such contractual relationship.

SECTION 3. Findings; principles of information practice.

(a) The General Assembly finds:

(1) That an individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;

(2) That the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;

(3) That an individual's opportunities to secure employment, insurance, credit and his or her right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and

(4) That in order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.

(b) Record-keeping agencies of the state and political subdivisions shall adhere to the following principles of information practice to ensure safeguards for personal privacy:

(1) There shall be no personal information system whose existence is secret.

(2) Information shall not be collected unless the need for it has been clearly established in advance.

(3) Information shall be appropriate and relevant to the purpose for which it has been collected.

(4) Information shall not be obtained by fraudulent or unfair means.

(5) Information shall not be used unless it is accurate and current.

(6) There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.

(7) There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.

(8) Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse.

(9) There shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose.

(10) The state or any agency or political subdivision thereof shall not collect personal information except as explicitly or implicitly authorized by law.

SECTION 4. Administration of systems including personal information.

(a) Any agency maintaining an information system that includes personal information shall:

(1) Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency;

(2) Collect information to the greatest extent feasible from the data subject directly;

(3) Establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

(4) Maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject;

(5) Make no dissemination to another system without (i) specifying requirements for security and usage including limitations on access thereto, and (ii) receiving reasonable assurances that those requirements and limitations will be observed, provided this subdivision shall not apply to a dissemination made

by an agency in another state, district or territory of the United States where the personal information is requested by the agency of such other state, district or territory in connection with the application of the data subject therein for a service, privilege or right under the laws thereof, nor shall this apply to information transmitted to family advocacy representatives of the United States Armed Forces;

(6) Maintain a list of all persons or organizations having regular access to personal information in the information system;

(7) Maintain for a period of three (3) years or until such time as the personal information is purged, whichever is shorter, a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority but excluding access by the personnel of the agency wherein data is put to service for the purpose for which it is obtained;

(8) Take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, about all the requirements of this chapter, the rules and procedures, including penalties for noncompliance, of the agency designed to assure compliance with such requirements;

(9) Establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security; and

(10) Collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects which is maintained, used or disseminated in or by any information system operated by any agency unless authorized explicitly by statute or ordinance.

SECTION 5. Violation of act; action for damages

Whenever there shall be a violation of this act, an application may be made by the Attorney General in the name of the state of Tennessee to a court having jurisdiction to issue an injunction, and upon notice to the defendant of not less than five (5) days, to enjoin and restrain the continuance of such violations; and if it shall appear to the satisfaction of the court that the defendant has, in fact, violated this section, an injunction may be issued by such court, enjoining and restraining any further violation, without requiring proof that any person has, in fact, been injured or damaged thereby.

Whenever the court shall determine that a violation of this section has occurred, the court may impose a civil penalty of not more than one thousand dollars (\$1,000) for each violation. In connection with any such proposed application, the Attorney General is authorized to take proof and make a determination of the relevant facts and to issue subpoenas in accordance with the civil practice law and rules.

SECTION 6. This act shall take effect upon becoming a law, the public welfare requiring it.